REMARKS

In response to the Official Action dated 3/13/2006, the above-identified application has been amended to place the claims in better condition for allowance and the added language finds basis in the specification at page 7, last paragraph of the Specification. Review and reconsideration are requested in view of the above amendments and following remarks.

In the Office Action of 3/13/2007, the Examiner states as follows:

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject mailer as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-19 are rejected under 35 U.S.C 103(a) as being unpatentable over Freed et al., us 2003/0014628 and further in view of Cast, us 2003/0046532.

In claims 1 and 11, Freed discloses a system and method for increasing data access in a secure socket layer network environment, which includes:

a web server computer having SSL protocol server software operably associated therewith for enabling a S5L connection, wherein SSL protocol server software includes a CA certificate and private key, 5SL acceleration server software operably associated with said web server computer which includes a pseudo CA certificate and access to said private key and a public key (paragraphs [0006140009], [0052]-[0053]); and

a client computer communicatively linked to said web server computer having web browser software having 5SL protocol client software operably associated therewith for enabling an SSL connection between said client and said web server, S5L acceleration device operably associated with said client computer which communicates with said SSL acceleration device to receive a copy of said pseudo CA certificate and said public key and present said pseudo CA certificate to said web browser software for validation thereof (paragraphs 100061100091, [0034]-[0035], [0052]-[0053]).

Freed et al. fail to disclose SSL acceleration being performed by client and server software. Gast discloses SSL acceleration being performed by client and server software (paragraph [0009]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Freed's secure communications method with Gast's acceleration system utilizing client and server software for acceleration to provide greater control by the client and server. It is for this reason that one of ordinary skill in the art would have been motivated to provide Freed's secure communications method with SSL acceleration performed by client and server software because it helps increase the speed at which encrypted network transactions may be processed (Gast, paragraph [0015]).

In claims 2 and 12, Freed, as modified, discloses the system and method of claims 1 and 11, respectively, wherein said SSL acceleration client software is further equipped for monitoring when said web browser requests a SSL connection with said we!) server computer and intercepting said SSL request from said web browser, and diverting communication through one of an established and an initiated SSL connection through said SSL acceleration client software and SSL acceleration server software (Freed, paragraphs [0034]-[0035], [0047]-[0048]).

In claims 3 and 13, Freed, as modified, discloses the system and method of claims 1 and 11, respectively, wherein said SSL acceleration client software is equipped to initiate a SSL request to said SSL acceleration server software operably disposed with web server computer to establish a SSL connection (Freed, paragraphs [0034]-[0035], [0047]-[0048]).

!n claims 4 and 14, Freed, as modified, discloses the system and method of claims 3 and 13, respectively, wherein SSL acceleration server software is further equipped for monitoring when the web server computer receives a request for a SSL connection through said SSL acceleration client software where upon such request initiates a SSL handshake wherein said pseudo CA certificate is sent to said client computer via SSL acceleration client software with a public key (Freed, paragraphs [0006]-[0009], [0052]-[0053]).

In claims 5 and 15, Freed, as modified, discloses the system and method of claims 4 and 14, respectively, wherein said web browser software is equipped to send a list of available encryption algorithms to said web server computer and said SSL acceleration client software intercepts said list, selects an encryption algorithm from said list (Freed, paragraphs [0008], [0034]-[0035], [0055]-[0056D.

In claims 6 and 16, Freed, as modified, discloses the system and method of claims 5 and 15, respectively, wherein said SSL acceleration client software is equipped to send

said chosen encryption algorithm to said browser software (Freed, paragraphs [0008], [0034]-[0035], [0055]-[0056]).

In claims 7 and 17, Freed, as modified, discloses the system and method of claims 6 and 16, respectively, wherein said browser software is equipped to create a secret key, encrypt using said chosen encryption algorithm and using said public key and send said encrypted secret key to said server computer through said SSL acceleration client software/ SSL acceleration server software (Freed, paragraphs [0007]-[0010]).

In claims 8 and 18, Freed, as modified, discloses the system and method of claims 7 and 17, respectively, wherein said SSL acceleration server software is equipped to de-encrypt said secret key using said private key (Freed, paragraphs [0007]-[001 0], [0034]-[0035]).

In claims 9 and 19, Freed, as modified, discloses the system and method of claims 8 and 18, respectively, which includes compression software for transmitting data secure communications between said client computer and said web server computer (Freed, paragraphs [0052]-[0053]).

In claim 10, Freed discloses a system for increasing data access in a secure socket layer network environment, which includes:

a web server computer having SSL acceleration server software for transferring a copy of a pseudo CA certificate and a public key (paragraphs [0006]-[0009], [0052]-[0053]); and

a client computer communicatively linked to the web server computer having SSL acceleration device operably associated with said client computer which communicates with said SSL acceleration device to receive said copy of a pseudo CA certificate and said public key and present said pseudo CA certificate to web browser software on said client computer for validation thereof (paragraphs [0006]-[0009], [0034]-[0035], [0052]-[0053]).

Freed fails to disclose SSL acceleration being performed by client and server software. Gast discloses SSL acceleration being performed by client and server software (paragraph [0009]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Freed's secure communications method with Gast's acceleration system utilizing client and server software for acceleration to provide greater control by the client and server. It is for this reason that one of ordinary skill in the art would have been motivated to provide Freed's secure communications method with SSL acceleration performed by client and server software because it helps increase the speed at which

encrypted network transactions may be processed (Gast, paragraph [0015].)

Applicants kindly traverse. Freed et al. discloses a secure sockets layer architecture which employs an intermediate device between the client computer and the server computer which intercepts SSL/TCP data and then performs one or more transactions to aid in acceleration. There is no direct link between the client computer and the server computer. As seen in paragraphs [0007-0010] of Freed et al., there is merely a conventional SSL handshake which is employed and all secure data is sent through the one secure tunnel which is created. Freed et al are concerned with offloading the server the task of encryption/decryption task by employing a tertiary or intermediary device to interact with the client and the server. Nevertheless, the tertiary computer employs conventional handshake technology.

This is very different from the instant invention. The present invention calls for a system for increasing data access in a secure socket layer network environment, which includes:

a web server computer having SSL protocol server software operably associated therewith for enabling a SSL connection, wherein SSL protocol server software includes a CA certificate and private key, SSL acceleration server software operably associated with the web server computer which includes a pseudo CA certificate and access to the private key and a public key; and

a client computer communicatively linked to said web server computer having web browser software having SSL protocol client software operably associated therewith for enabling a first SSL connection between the client and the web server, SSL acceleration client software operably associated with the client computer which communicates with the SSL acceleration server software to receive a copy of the pseudo CA certificate and the public key and present the

pseudo CA certificate to the web browser software for validation thereof for enabling a second SSL connection between the client and the server in a manner which permits optimization techniques to be performed on data transmitted through the second SSL connection. A method employing these elements is also provided.

The instant invention provides a server with SSL protocol server software and SSL acceleration server software on both the client and server for enabling direct and multiple SSL sessions to take place through the use of creating a pseudo CA certificate on the web server in addition to having the existing CA certificate on the web server which are presented to the client computer having SSL protocol and SSL acceleration software thereon. By so providing, multiple direct secure links are created. Freed et al. introduces a third element in the chain of connection and another potential break point for communication.

The instant invention enables secure data be transacted using the CA certificate from the web server over an initial SSL connection for transacting key data which must pass over such connection, such as when connecting to a secure bank site, for example. In addition, the instant invention provides the pseudo CA certificate and secondary SSL connection through which data may pass in a secure connection which permits functional operations to be performed thereon, such as compression of data. This is not taught, disclosed or suggested in Freed et al. and this can't be accomplished in the teachings of Freed et al. Freed et al. only acts as an intermediary intercepting all communication over the existing SSL connection and passes the data accordingly, paragraph [0039]. Paragraphs [0052] - [0053] and the claims in Freed et al. further illustrate Freed et al. are only concerned with providing a classic SSL connection between the client and server through an intermediary device.

Gast is directed to a system and method for accelerating cryptographically secured transactions. Gast is concerned with offloading encryption processing to central encryption servers equipped with hardware built to accelerate encryption speed and reduce latency [paragraph 0015]. Gast simply moves the task of processing the security mechanism, i.e., establishing a SSL session to a central control point [0022]. The point stressed in Gast is to offload the establishment of SSL connections by the server, not to establish additional SSL connection between the client and server as opposed to the instant invention which provides a CA certificate and a pseudo CA certificate to establish concurrent SSL connections through whereby data can bass in a compressed form, for example, in the second established connection. Gast teaches away from the instant invention.

It is respectfully submitted that the instant claimed invention is not taught, disclosed or suggested by Gast or Freed et al. taken alone or together. The instant invention is respectfully submitted to be patentably distinct over the art of record. Withdrawal of the rejection of claims 1-19 is respectfully requested.

Therefore, allowance of claims 1-19 is requested at as early a date as possible. This is intended to be complete response to the Official Action dated 3/13/2007 and a one month extension is requested and this is considered a Petition for Extension therefor.

Respectfully submitted,

/R. William Graham/

R. William Graham, 33,891

Certificate of Transmission

I hereby certify that this correspondence is being electronically filed with the PTO for

group 2137on the date shown below.

/R. William Graham/

Date. Friday, July 13, 2007 R. William Graham, 33,891